REMARKS

This submission is a full and timely response to the aforementioned Office Action. By this amendment, Applicants have amended the abstract and specification to correct an error in translation. Moreover, claims 1, 2, and 4 have been amended to be more consistent with the amended specification. No new matter has been added. Claims 1-4 are pending.

Objections to the Specification

The Office Action alleges that the specification and claims of the instant application are not consistent with a translation of the abstract of priority document JP 11-231683. Applicants have provided a substitute specification with marked-up changes that address and remedy those issues raised by the Office Action. In particular, Applicants have changed each instance of "read hysteresis information" to "read history information," which is consistent with language used in the priority document. Applicants respectfully submit that the substitute specification contains no new matter. Moreover, Applicants thank the Examiner for identifying inconsistencies between the disclosure of the instant application and the disclosure priority document, and for providing suggestions in correcting the same.

Rejections Under 35 U.S.C. §112

Claims 1-4 were rejected under 35 U.S.C. §112, first paragraph. Applicants have amended claims 1 and 4 to address and remedy the issues raised by the Office Action. In particular, each of claims 1 and 4 have been amended to replace "read hysteresis information" with "read history information." Thus, Applicant respectfully requests that the rejection to claims 1-4 under §112, first paragraph be withdrawn.

Rejections Under 35 U.S.C. §103

Claims 1-4 were rejected under 35 U.S.C. §103 as unpatentable over *Matsumura*, U.S. Patent No. 5,493,621, in view of *Hirakawa et al.*, U.S. Patent No. 5,664,126.

Claim 1 recites a fingerprint collating device for collating a user's fingerprint with registered fingerprint information to effect personal authentication, said device comprising, a fingerprint reader reading said fingerprint to create read fingerprint information, and to create read history information indicating that said read fingerprint information has been created; a , i.e. history read history storage for storing said read history information; and a collator for collating said read fingerprint information with said registered fingerprint information to effect personal

authentication and output a result of authentication when said read history information is stored in said read history storage.

Claim 4 recites a fingerprint collating method for collating a user's fingerprint with registered fingerprint information to effect personal authentication, said method comprising the steps of, reading said fingerprint to create read fingerprint information, and to create read history information indicating that said read fingerprint information has been created; storing said read history information in read history storing means; and collating said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said read history information is stored in said read history storing means.

Matsumura discloses a fingerprint ID system 10 and method for comparing fingerprint image data with registered or previously stored image data in real time. *See* col. 3, lines 37-41. To compare fingerprint data the fingerprint image input device 11 receives a fingerprint image when a finger is placed on a sheet of transparent glass. The received image is stored in the frame memory 13. The acquired image is thinned and minutia is extracted. The image is then registered based on positions of branch points of the minutae. The degree of mismatch between the branch points in the image and registered data is generated to determine the whether the image data matches the registered data. A mismatching value below a predetermined value indicates that the image data and registered data are a match. When a recognition rate for the image data is below a predetermined value, a template matching method is then used. The Office Action acknowledges that *Matsumura* does not disclose how the read hysteresis management is performed, and based on the current claim amendments Applicants submit *Matsumura* fails to disclose how read history management is performed.

Hirakawa discloses a human interface system constructed by connecting systems containing a plurality of computers or workstations via a local or wide area network includes site building means for building a plurality of sites that either retain or manage a plurality of pieces of data and a plurality of programs. *See* Abstract. Each computer on the network contains at least one program known as an agent. A user may send a message to an agent via an input to the computer. The agent may then respond to the user's message by presenting information to a display of the user. The various agents are capable of execution on the computer in which it is stored, and on any other computer connected to the network. *See* col. 11, lines 1-9. A computer, acting defined as a site server on the network, manages a number of virtual sites, and executes processes that creates, updates, or deletes agents with respect to that particular site. Based on

virtual site definitions specified by a user at a client computer the site server creates an agent corresponding to the user's definition. These virtual sites have structures corresponding to a department store or office containing, for example, a desk, file cabinet, clock, and telephone. *See* col. 11, lines 44-65.

To move an agent within a virtual site, *Hirakawa* discloses that the user sends positional information or commands to the agent. Based on this information the position of the agent is adjusted. On the other hand, when moving an agent between two virtual sites, *Hirakawa* discloses that site link information of a virtual site is retrieved and stored by a user. Site hysteresis information, which is a combination of a virtual site's name and ID and contains the hysteresis of the sites that the person has visited, is then held by the user. The user may enter a specified key or code, e.g., a phone number to retrieve the site ID, natural language, or postal code. *See* col. 17, line 12 – col. 18, line 16. At the site server, the site hysteresis information may be collated with information related to a current message of a user, to determine whether that same site was previously visited or retrieved. *See* col. 45, lines 41-55.

In contrast, claim 1 recites, among other things, a collator for collating said read fingerprint information with said registered fingerprint information to effect personal authentication and output a result of authentication when said read history information is stored in said read history storage. The read history information of the instant invention indicates whether a finger is been placed on the prism 50 and a fingerprint is successfully read and stored. Thus, collation is not executed until image data D37 of the fingerprint is created. In addition, the read history information does not determine whether that same finger has been previously read.

Neither *Matsumura* nor *Hirakawa* discloses, teaches, or suggests at least a collator as noted above. Instead, *Matsumura* discloses that a fingerprint image is compared to a registered fingerprint image, but fails to disclose or suggest that the collation of the fingerprint images is predicated on whether read history information is stored. In particular, *Hirakawa* discloses the use of site hysteresis information in obtaining an ID of a virtual site, wherein the site hysteresis information contains the hysteresis of the sites that a user has visited. Thus, Applicants submit that the site hysteresis information and storage of *Hirakawa* is not related or analogous to the read history information and storage of the instant invention. Furthermore, the teachings of *Hirakawa* are not related to fingerprint registration, or identification, and neither discloses, teaches, nor suggests a motivation for using such a technique for these purposes. Nor are these teachings directed or related to the same problem resolved by the instant invention.

To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Moreover, obviousness "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys. V. Montefiore Hosp., 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984).

It is established law that one "cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." Ecolochem, Inc. v. Southern California Edison Company, page 23, September 7, 2000 (Fed. Cir.) (citing In re Fine, 837 F.2d 1071, 1075, 5, USPQ2d 1780, 1783 (Fed. Cir. 1988)). "Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability—the essence of hindsight." Ecolochem at 24 (citing In re Dembiczak, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999)). "When a rejection depends on a combination of prior art references, there must be some teaching, suggestion, or motivation to combine the references." Ecolochem at 24 (citing In re Rouffet, 149 F.3d 1350, 1355, 47 USPQ2d 1453, 1456 (Fed. Cir. 1988), citing In re Geiger, 815 F.2d 686, 688, 2 USPQ2d 1276, 1278 (Fed. Cir. 1987)). Additionally, "defining the problem in terms of its solution reveals improper hindsight in the selection of the prior art relevant to obviousness." Ecolochem at 24 (citing Monarch Knitting Mach. Corp. v. Sulzer Morat Gmbh, 139 F.3d 877, 880, 45 USPQ2d 1977, 1981 (Fed. Cir. 1998)).

Based on the foregoing discussion, Applicant submits that *Matsumura* and *Hirakawa* either singly or combined, fail to disclose, teach, or suggest at least a least a collator as recited above. In particular, the combination of the aforementioned references lacks the requisite motivation and rises to the level of hindsight reasoning. Thus, Applicant respectfully requests that the rejection of claim 1 under 35 U.S.C. §103 should be withdrawn, and this claim allowed.

Claims 2 and 3 depend from claim 1. By virtue of this dependency, Applicants submit that claims 2 and 3 are allowable for at least the same reasons given above with respect to claim 1, and are further distinguished over *Matsumura* and *Hirakawa* by each respective claim combination. Applicants respectfully request, therefore, that the rejection of claims 2 and 3 under 35 U.S.C. §103 be withdrawn, and these claims be allowed.

Based on the foregoing discussion, Applicants further submit that with respect to independent claim 4, the Office Action has also not established a *prima facie* case for obviousness. Thus, Applicants respectfully request that the rejection of claim 4 under 35 U.S.C. §103 be withdrawn, and claim 4 be allowed.

Conclusion

Based on at least the foregoing amendments and remarks, Applicants submit that claims 1-4 are allowable, and this application is in condition for allowance. Accordingly, Applicants request favorable reexamination and reconsideration of the application. In the event the Examiner has any comments or suggestions for placing the application in even better form, Applicants request that the Examiner contact the undersigned attorney at the number listed below.

Dated: June 18, 2003

Respectfully submitted,

By_____
Ronald P. Kananen
Registration No.: 24,104
Attorneys for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building
1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353

In the event additional fees are necessary in connection with the filing of this paper, or if a petition for extension of time is required for timely acceptance of same, the Commissioner is hereby authorized to charge Deposit Account No. 180013 for any such fees; and applicants hereby petition for any needed extension of time.

FINGERPRINT COLLATING DEVICE AND FINGERPRINT COLLATING METHOD

BACKGOUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to a fingerprint collating device and a fingerprint collating method, and more particularly, is suitably applied to a fingerprint collating device to effect personal authentication by using the fingerprint, for example.

DESCRIPTION OF THE RELATED ART

Conventionally, there is a fingerprint collating unit for effecting personal authentication by using the fingerprint. Such fingerprint collating unit uses an image pick-up element to photograph a user's fingerprint, and produce a fingerprint image. And the fingerprint collating unit collates the photographed fingerprint image with the registered fingerprint image for collation to effect personal authentication. The fingerprint is unchanged throughout one's life and different from person to person. Therefore, the fingerprint can securely assure the personal authentication.

However, the third party may pick up the other's fingerprint from a cup or the like, for example, to falsify a fingerprint image, and enter the falsified fingerprint image into the fingerprint collating unit for the fingerprint collation. The third party may abuse the falsified fingerprint for personal authentication.

SUMMARY OF THE INVENTION

In view of the foregoing, an object of this invention is to provide a fingerprint collating device and a fingerprint collating method which can prevent an illicit use of the other's fingerprint.

The foregoing object and other objects of the invention have been achieved by the provision of a fingerprint collating device for collating a user's fingerprint the registered fingerprint information to effect personal authentication, comprising fingerprint reader for reading the user's fingerprint to create read fingerprint information, and to create read ~~hysteresis~~history information indicating that the read fingerprint information has been created, read ~~hysteresis~~history storage for storing the read ~~hysteresis~~history information, and collator for collating the read fingerprint information with the registered fingerprint information to effect personal authentication and output a result of authentication when the read ~~hysteresis~~history information is stored in the read ~~hysteresis~~history storage.

The read ~~hysteresis~~history information indicating that the read fingerprint information has been created is stored in the read ~~hysteresis~~history storage, and the read fingerprint information is collated with the registered fingerprint information to effect personal authentication when the read ~~hysteresis~~history information is stored in the read ~~hysteresis~~history storage. Therefore, even if the read fingerprint information is improperly entered from the outside, the personal authentication is not effected, leading to prevention of an illicit use.

The nature, principle and utility of the invention will become more apparent from the following detailed description when read in conjunction with the accompanying drawings in which like parts are designated by like reference numerals or characters.

BRIEF DESCRIPTION OF THE DRAWINGS

In the accompanying drawings:

Fig. 1 is a block diagram showing the configuration of a fingerprint collation system according to the present invention;

Fig. 2 is a block diagram showing the configuration of a fingerprint collating unit; and

Fig. 3 is a diagram showing a stored state of fingerprint data.

DETAILED DESCRITION OF THE EMBODIMENT

Preferred embodiments of this invention will be described with reference to the accompanying drawings:

(1) Overall Configuration of a Fingerprint Collation System

In Fig. 1, reference numeral 1 denotes a fingerprint collation system of the invention as a whole, in which a card reader 20 for reading or writing data from or to an Integrated Circuit (IC) card 21 and a fingerprint collating unit 30 as a fingerprint collating device are connected to a personal computer 10. The personal computer 10 is connected to the card reader 20, as well as the fingerprint collating unit 30, via an RS-232C serial interface.

The fingerprint collating unit 30 accepts a user's fingerprint, and collates the fingerprint with either a fingerprint template (reference fingerprint data for the person for authentication) registered in the fingerprint collating unit 30 or a fingerprint template registered in the IC card 21, a result of fingerprint collation being output to the personal computer 10.

The fingerprint collating unit 30 has a plurality of fingerprint templates registered, each fingerprint template being identified by an index number N index. Also, the IC card 21 has a fingerprint template of an owner of the IC card 21 registered.

(2) Fingerprint Registration Process

When the fingerprint of a person for authentication is registered in the fingerprint collating unit 30, the personal computer 10 sends a fingerprint registration instruction Reg and an index number N index specified by the user to the fingerprint collating unit 30 in response to the fingerprint registration operation of the user.

Fig. 2 is a diagram of the fingerprint collating unit 30 as a whole. A CPU 31, a program Random Access Memory (RAM) 32, a program flash Read Only Memory (ROM) 33, and a collation controller 34 are connected to a main bus 39. The CPU 31 reads a control program from the program flash ROM 33 and executes the control program in the program RAM 32 to control the whole of the fingerprint collating unit 30.

That is, the CPU 31 receives the fingerprint registration instruction Reg and the index number N index sent from the personal computer 10 via a RS232C driver 38. And the CPU 31 controls the collation controller 34 in accordance with the fingerprint registration instruction Reg to start reading the fingerprint.

The collation controller 34 turns on an LED 41 under the control of the CPU 31 to apply an illuminating light L1 onto the bottom face of a prism 50. Then, the user puts one's finger with fingerprint face to be registered on the slant of the prism 50 firmly.

The prism 50 reflects the illuminating light L1 on the interior of the slant of prism to cause a reflected light L2 to be outgoing via a lens (not shown) provided within a lens barrel 51 to a Charge Coupled Device (CCD) 40. The prism 50 reflects totally the illuminating light L1, when there is an air layer on the outer face of the slant, while diffusing the illuminating light L1, when there is no air layer on the outer face of the slant. Therefore, when the user puts one's

finger with fingerprint face firmly on the slant of the prism 50, the illuminating light L1 is reflected at a concave portion of the fingerprint due to the presence of air layer, while being diffused at a convex portion of the fingerprint due to the absence of air layer. Consequently, the reflected light L2 results in an image which is bright in the concave portion of fingerprint and dark in the convex portion of fingerprint. The CCD 40 produces an image signal S40 by picking up the reflected light L2, and outputs the image signal S40 to an analog/digital converter 37. In this way, the fingerprint is optically read.

The analog/digital converter 37 converts the image signal S40 into a digital signal, which is binarized and output as the fingerprint image data D37 to the collation controller 34. At this time, the collation controller 34 displays the fingerprint image data D37 via the RS232C driver 38 on a monitor 11 of the personal computer 10 (Fig. 1). Thereby, the user confirms one's own fingerprint photographed to adjust the disposition of the finger with respect to the prism 50.

The collation controller 34 extracts the feature points of fingerprint (central or branch point of fingerprint pattern) from the fingerprint image data D37 to produce a fingerprint template Temp. And the collation controller 34 registers the fingerprint template Temp and an attribute Attb associated with the fingerprint template Temp at an index (address) specified by the index number N index within the collation flash ROM 35, as shown in Fig. 3, and notifies the personal computer 10 that the registration of fingerprint has been completed (Fig. 1).

(3) Fingerprint Collation Process

(3-1) Fingerprint collation process with fingerprint template within fingerprint collating unit

When the fingerprint collation is performed by using a fingerprint template Temp registered within the fingerprint collating unit 30, the user uses the personal computer 10 to start

a fingerprint collation process and input an index number N index. The personal computer 10 sends a fingerprint collation instruction Ref and the index number N index specified by the user to the fingerprint collating unit 30 in response to this.

In Fig. 2, the CPU 31 receives the fingerprint collation instruction Ref and the index number N index sent from the personal computer 10 via the RS232C driver 38, controls the collation controller 34 in accordance with the fingerprint collation instruction Ref to start reading the fingerprint.

The collation controller 34 turns on the LED 41 under the control of the CPU 31, like when registering the fingerprint, and applies an illuminating light L1 on the bottom face of the prism 50. At this time, the user puts one's finger with fingerprint face on the slant of the prism 50 firmly.

The prism 50 reflects the illuminating light L1 at the interior of the slant of prism, and causes the reflected light L2 representing the user's fingerprint image to be outgoing via a lens (not shown) provided within the lens barrel 51 to the CCD 40 which is fingerprint reading means. The CCD 40 picks up the reflected light L2 to produce an image signal S40 for output to the analog/digital converter 37. The analog/digital converter 37 converts the image signal S40 into a digital signal, which is binarized and output as the fingerprint image data D37 to the collation controller 34.

Here, when the fingerprint image data D37 is normally produced, the collation controller 34 which is fingerprint reading means sets a fingerprint accepting flag as reading ~~hysteresis~~history information indicating that the fingerprint has been read in the program RAM 32 which is reading ~~hysteresis~~history storing means.

And the collation controller 34 as collating means reads the fingerprint template Temp specified by the index number N index from the collation flash ROM 35 and collates the fingerprint image data D37 with the read fingerprint template Temp.

At this time, the collation controller 34 executes the collation between the fingerprint template Temp and the fingerprint image data D37, only when the fingerprint accepting flag has been set in the program RAM 32, but does not execute the collation when the fingerprint accepting flag has not been set in the program RAM 32. Namely, the fingerprint collating unit 30 performs the collation of fingerprint only with the fingerprint image data D37 read by the fingerprint collating unit 30, but does not perform the collation of fingerprint even if the fingerprint image data D37 is input externally. Thereby, it is possible to prevent an illicit use of fingerprint, using the falsified fingerprint image data.

After the collation between the fingerprint template Temp and the fingerprint image data D37 has been completed, the collation controller 34 resets the fingerprint accepting flag in the program RAM 32, and outputs a result of collation to the personal computer 10 (Fig. 1).

(3-2) Fingerprint collation process with fingerprint template within IC card

When the collation of fingerprint is made using the fingerprint template Temp registered within the IC card 21, the user inserts the IC card 21 into the card reader 20, and uses the personal computer 10 to start the fingerprint collation operation. The personal computer 10 sends a fingerprint collation instruction Ref to the fingerprint collating unit 30 in response to this.

The CPU 31 (Fig. 2) controls the collation controller 34 in accordance with the fingerprint collation instruction Ref to start reading the fingerprint. The collation controller 34 reads a user's fingerprint to produce the fingerprint image data D37 and store it in the collation

RAM 36 under the control of the CPU 31, like when registering the fingerprint. Herein, when the fingerprint image data D37 can be normally produced, the collation controller 34 sets the fingerprint accepting flag indicating that the fingerprint has been read in the program RAM 32.

The collation controller 34 reads the fingerprint template Temp registered within the IC card 21 via the personal computer 10, and stores the fingerprint template Temp at an index #0 in the collation flash ROM 35. And the collation controller 34 reads the fingerprint template Temp from the index #0 in the collation flash ROM 35, and performs the collation between the fingerprint template Temp and the fingerprint image data D37.

At this time, the collation controller 34 executes the collation between the fingerprint template Temp and the fingerprint image data D37, only when the fingerprint accepting flag has been set in the program RAM 32, but does not execute the collation when the fingerprint accepting flag has not been set in the program RAM 32.

After the collation between the fingerprint template Temp and the fingerprint image data D37 has been completed, the collation controller 34 resets the fingerprint accepting flag in the program RAM 32, and outputs a result of collation to the personal computer 10 (Fig. 1).

(4) Operation and Effect

In the above configuration, the fingerprint collating unit 30 accepts a user's fingerprint to produce the fingerprint image data D37. At this time, when the fingerprint image data D37 is normally produced, the collation controller 34 sets the fingerprint accepting flag in the program RAM 32.

And the collation controller 34 performs the collation between the fingerprint template Temp within the fingerprint collating unit 30 or the IC card 21 and the fingerprint image data D37, only when the fingerprint accepting flag has been set in the program RAM 32.

With the above configuration, the fingerprint accepting flag is set when the user's fingerprint is accepted to produce the fingerprint image data D37. Only when the fingerprint accepting flag has been set, the collation of fingerprint is performed. Therefore, even if the fingerprint image data D37 is entered externally into the fingerprint collating unit 30, the collation of fingerprint is not performed. Consequently, it is possible to prevent an illicit use of fingerprint, using the falsified fingerprint image data.

As described above, according to the present invention, the read ~~hysteresis~~history information representing that the read fingerprint information has been produced is stored in the read ~~hysteresis~~history storing means. When the read ~~hysteresis~~history information is stored in the read ~~hysteresis~~history storing means, the collation between the read fingerprint information and the registered fingerprint information is performed to effect personal authentication. Even if the read fingerprint information is entered externally and illicitly, the personal authentication is not performed. Consequently, it is possible to provide the fingerprint collating device which can prevent an illicit use of fingerprint.

While there has been described in connection with the preferred embodiments of the invention, it will be obvious to those skilled in the art that various changes and modifications may be aimed, therefore, to cover in the appended claims all such changes and modifications as fall within the true spirit and scope of the invention.